IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

GENESCO, INC.,	)	
	)	
Plaintiff,	)	Case No. 3:13-0202
	)	Chief Judge Haynes
v.	)	
	)	
VISA U.S.A., INC., VISA, INC., and VISA INTERNATIONAL SERVICE ASSOCIATION,	)	
	)	
Defendants.	)	

AMENDED MEMORANDUM

Plaintiff, Genesco Inc., a Tennessee corporation, filed this action under 28 U.S.C. § 1332, the federal diversity jurisdiction statute, against the Defendants: Visa U.S.A. Inc., Visa Inc., and Visa International Service Association (collectively "Visa"), Delaware corporations with their principal places of business in California. Genesco asserts state law claims against the Visa Defendants arising out of Visa's assessments of $13,298,900.16 in non-compliance fines and reimbursement assessments after a cyber attack involving credit and debit card purchases at Genesco's retail establishments. Visa imposed these assessments against Wells Fargo Bank, N.A. and Fifth Third Financial Corporation under Visa's agreements with those Banks to process retail purchases with Visa credit and debit cards. Wells Fargo and Fifth Third had separate agreements with Genesco to process Visa credit and debit card transactions for purchases at Genesco's retail establishments. Wells Fargo and Fifth Third also had indemnification agreements with Genseco under which Genesco agreed to indemnify Fifth Third and Wells Fargo for the Banks' losses incurred in processing Visa credit and debit card transactions with Genesco's retail establishments. Fifth Third

and Wells Fargo collected Visa's fines and assessments from Genesco. For this action, Genesco is the assignee and subrogee of Fifth Third and Wells Fargo for any claims of those Banks against Visa for these fines and assessments.

Genesco asserts multiple claims for Visa's alleged breaches of contracts and implied covenants of good faith and fair dealing in imposing and collecting these fines and assessments. Genesco also asserts claims under the California Unfair Competition Act, Cal. Bus & Prof. Code §17200 et seq. and common law claims of unjust enrichment and restitution. The specifics of Genesco's claims are, in essence, that Visa's fines and assessments against the Banks lack a factual basis and were imposed in violation of Visa's Visa International Operating Regulations ("VIOR") that are incorporated into Visa's agreements with Wells Fargo and Fifth Third. Genesco seeks recovery of Visa's fines and assessments against the Banks as well as incidental damages incurred by these Banks and Genesco due to Visa's alleged wrongful conduct in imposing and collecting these fines and assessments. In earlier proceedings, the Court denied Visa's motion to dismiss Genesco's claims under the California Unfair Competition Act, Cal. Bus & Prof. Code §17200 et seq. and common law claims of unjust enrichment and restitution. (Docket Entry Nos. 49 and 50).

Before the Court are the following discovery motions: Genesco's motion for a protective order (Docket Entry No. 88), Visa's motion to compel (Docket Entry No. 120) and Genesco's motions for protective order concerning Visa's subpoena to Genesco's expert consultant and Visa's deposition notice for Genesco's general counsel. (Docket Entry Nos. 201 and 235). The Court held a discovery hearing on these motions that raise common or overlapping issues about the scope of appropriate discovery in this action. Given the complexity of the issues raised in the motions, the Court circulated a draft Memorandum and granted leave for the parties' counsel to review and

comment. The Court also granted the parties leave to file supplemental memoranda. The parties submitted multiple memoranda as well as multiple affidavits. See Docket Entry Nos. 221, 227, 229, 241, 253, 275, 278 and 296.

In sum, Genesco contends that this controversy involves whether Visa's determinations that Genesco committed the four security violations have factual bases to justify Visa's imposition of the fines and assessments. Genesco alleges that Visa lacked a factual basis for these fines and assessments and thereby breached Visa's contracts with Wells Fargo and Fifth Third, as well as the legal obligations owed directly to Genesco. In addition, Genesco asserts that under Visa's VIOR, Visa may look only to the facts relied upon by Visa in assessing fines or reimbursement costs. Thus, Genesco deems Visa's discovery requests for all aspects of Genesco's computer system to be irrelevant and barred by California law as well as the attorney client and work product privileges. Based upon the prior investigation of Genesco's computerized payment network compliance at Visa's behest, Genesco contends that Visa's discovery requests are unduly burdensome and request irrelevant information. Genesco also challenges Visa's discovery requests and subpoena to the Stroz firm, its nontestifying expert consultant, as barred by Fed. R. Civ. P. 26(b)(4)(D) absent a showing of requisite extraordinary circumstances that Visa has not made. Genesco also asserts the attorney client and work product privileges as barring the depositions of its general counsel and expert consultant.

For its contentions, Visa asserts, in essence, that Genesco's complaint repeatedly alleges Genesco's compliance with all computer security requirements that justifies discovery of Genesco's entire computer network for compliance with Visa's VIOR, including Genesco's remediation of its computer system after the cyber attack. Visa also contends that Genesco waived any privilege by

failing to file a privilege log and cites Genesco's voluntary disclosures of its consultant's findings. As to Genesco's general counsel,Visa cites the affidavits submitted by Genesco's counsel in this action and contends that Genesco's general counsel is the sole source of information on Genesco's theory of rebooting that is asserted to invalidate the factual predicates for Visa's fines and assessments.

A. Factual Background[1]

1. The Cyber Attack and Visa's Assessments

Between December 2009 and December 2010, a cyber attack occurred on Genesco's computer network that targeted payment card data on Genesco's computer network for its retail establishments throughout the world. (Docket Entry No. 1, Complaint at ¶ ¶ 17-22 and Docket Entry No. 121, Exhibit B to Carrillo Affidavit at 3). Specifically, intruders installed software onto Genesco's computer network to obtain cardholders' unencrypted account data as that data was transmitted to Wells Fargo or Fifth Third for payment authorizations. Id.

On June 1, 2010, Visa provided Wells Fargo its Common Point of Purchase ("CPP") report on Genesco. This report revealed that Issuers of Visa cards sent CPP reports about multiple accounts subjected to fraudulent activity, with Genesco as the common point of purchase. (Docket Entry Nos. 188-1 and 188-2, Edwards Affidavit, Exhibits B and C thereto). CPP reports continued for the next several months. (Docket Entry No. 188-3, Edwards Affidavit, Exhibit D thereto). On June 1, 2010,

[1] This section is necessary to place the parties' discovery disputes in an appropriate context. This section does not constitute findings of fact. "The first step in the resolution of any legal problem is ascertaining the factual background and sifting through the facts with an eye to the legally relevant." Upjohn Co v. United States, 449 U. S. 383, 390-91 (1981) (attorney-client privilege controversy). The Court cannot understand the parties' contention without a review of the factual record and deems it necessary to consider the text of relevant documents, as opposed to counsel's characterizations of those documents.

Visa requested Wells Fargo to submit a questionnaire to Genesco about these activities that Wells Fargo initiated. (Docket Entry No. 188-1, Edwards Affidavit, Exhibit B thereto). On October 25, 2010, Visa recommended that Wells Fargo conduct a forensic investigation. (Docket Entry No. 188-3, Exhibit D to Edwards Affidavit).

Citing Wells Fargo's and Fifth Third's obligations under the VIOR to ensure their merchants' compliance with Visa's computer security requirements, Visa required Fifth Third and Wells Fargo to submit validation and documentation of Genesco's compliance with their Payment Card Industry Data Security Standards ("PCI DSS") by a Qualified Security Assessor. Visa also required a quarterly network vulnerability scan and a completed attestation of Genesco's compliance. (Docket Entry Nos. 125 and 126, Carillo Affidavit, Exhibits F and G thereto). Fifth Third submitted this documentation on behalf of Genesco on June 29, 2011, and Wells Fargo did so on July 6, 2011. (Docket Entry Nos. 127-128, Carrillo Affidavit, Exhibits H and I thereto).

Earlier, on November 2, 2010, Genesco retained Trustwave International Security and Compliance ("Trustwave") to conduct a forensic investigation of the cyber attack that the parties refer to as the "Intrusion." (Docket Entry No. 91, Sisson Affidavit at ¶ 4).[2] Trustwave is among the firms listed as PCI Forensic Investigators ("PFIs") that are approved by the PCI Security Standards Council to conduct forensic computer investigations. On November 30, 2010, Trustwave commenced its on-site investigation at Genesco's computer facilities, namely, "to physically inspect and assess the following:

- Four Payment Switches

[2]Visa insists that it did not direct Genesco or its Acquiring Banks to select Trustwave. (Docket Entry No. 184 at 10 n.1)

- Four Windows Active Directory Domain Controllers
- Physical Security
- Network Topology"

(Docket Entry No. 104 at 7).

On January 27, 2011, Trustwave submitted its Incident Response Final Report that found Genesco noncompliant on three of twelve PCI DSS requirements at the time of fraudulent activities and that each deficiency contributed to the Intrusion. (Docket Entry No. 104 at 37). Trustwave's Report also noted some security deficiencies. Id. at 14. The specific "Secutity Deficiencies" found by Trustwave were listed as follows:

> 4.3 Security Deficiencies
> Through the onsite assessment, Genesco personnel interviews, and analysis, Trustwave discovered the following system and network security deficiencies:
>
> 1. Network Segmentation
>
> a) The PCI Zone was not fully segmented from the Genesco WAN; port 3389 (RDP) was configured to allow internal remote access from systems outside of the PCI Zone.
>
> b) Inbound and outbound access from the PCI Zone was not fully configured.
>
> 2. Remote Access
>
> a) The remote access solution for third-party vendor accounts was persistently enabled; remote access for third-party accounts should be only accessible only on an as-needed basis and enforce two-factor authentication.
>
> 3. File Integrity Monitoring
>
> a) File integrity monitoring software was not configured to monitor the Windows System32 directory.

Id. at 14-15. Genesco describes the Trustwave report as finding four violations of 3 PCI DSS or VIOR requirements: Requirement 1, 8 (two violations) and 11. (Docket Entry No.181 at 5-6, Harrington Affidavit, Exhibit X thereto). The Trustwave Report recommended several remedial measures and confirmed that Genesco installed those remedial measures onto its computer system. (Docket Entry No. 104 at 32-33).

Based on the Trustwave report with the PCI DSS violations, Visa determined that the Intrusion qualified under Visa's Account Data Compromise Recovery ("ADCR") and Data Compromise Recovery Solution ("DCRS") programs. (Docket Entry Nos. 122-24, Exhibits C, D and E to Carrillo Affidavit). Visa found as follows:

> **Evidence of Compromise**
>
> The forensic report provided by Trustwave found conclusive evidence that an account compromise event occurred. The report concluded the following:
>
> - There were 3 PCI violations. (Forensic Report, p. 37)
> - Evidence analyzed by Trustwave indicates that an address based in Belarus logged into the Genesco network with a vendors VPN account. This account then used RDP to remotely access the payment switches and installed network-packet capture malware to capture track data as it was sent through the system for authorization. (Forensic Report, p. 3)
> - Through analysis Trustwave is able to confirm that the earliest the malware was running on the impacted credit switches was December 4, 2009. Furthermore, Trustwave is able to determine the user account that the attacker used (orasvc) and confirm that the attacker was connected externally via a VPN account. (Forensic Report, p. 16)
> - VPN and domain controller logs indicate the attacker accessing the cardholder data environment. (Forensic Report, p. 27)
> - Analysis revealed the presence of network sniffing malware active on all four payment switches (Forensic Report, p. 14)

- The malware installed by the attackers was a version of tcpdump.exe, network sniffing malware, which was installed and renamed to look like a legitimate system application service on December 4, 2009 and removed on December 1, 2010. (Forensic Report, p. 23)

- Attacker aggregates malware output into multipart rar archive. ,(Forensic Report, p. 27)

- Trustwave was able to determine that the malware output contained restricted cardholder data. In this malware output, Trustwave was able to determine that several pieces of cardholder information were exposed, for both cards which were swiped and those that were manually typed at retail locations. (Forensic Report, p. 20)

The PCI DSS Violations indicated as "Not In Place" on page 7 could have allowed a compromise to occur.

(Docket Entry No. 99 at 7).

Visa assessed Wells Fargo and Fifth Third Bank in excess of $13 million in addition to $10,000 in fines for failing to ensure Genesco's PCI DSS compliance. (Docket Entry Nos. 122-126, Exhibits, C, D, E, F and G thereto Carrillo Affidavit). The assessments were represented as reimbursements to Visa's issuing Banks for their counterfeit fraud and associated operating expenses and losses. Id. As discussed infra, under Visa's VIOR, any assessments of fines and reimbursements must be based upon facts known to Visa. (Docket Entry Nos. 122-124, Carrillo Affidavit, Exhibits C, D, and E thereto).

Under Visa's VIOR, Fifth Third and Wells Fargo could appeal these fines and assessments and the Banks requested extensions to appeal to allow the Banks and Genesco to request information to determine whether to appeal under the VIOR process or to initiate litigation after Visa collected the fines and assessments. (Docket Entry Nos. 151-1 at 10-11, 159 at 1, 161 at 1, 181 at 11 and 182 at 8). Sometime in March 2011, Genesco provided Wells Fargo and Fifth Third Bank with an annotated response to the Trustwave report challenging Trustwave's findings of Genesco's

noncompliance with the three cited PCI DSS requirements under Visa's VIOR. Genesco argued that there were not any security deficiencies in Genesco's computer system. (Docket Entry No 129, Carrillo Affidavit, Exhibit J thereto at 4 citing (Comment [A34]), 5 (Comment [A55]), and 7 (Comments [A80]-[A83]).

In a July 11, 2011 document entitled "Visa review of Genesco's PCI DSS violations Trustwave report dated January 27, 2011", Ingrid Beierly, a Visa employee wrote:

> Trustwave identified the following PCI DSS violations:
>
> **Requirement 1 - Install and maintain a firewall configuration to protect cardholder data**
>
> Trustwave findings indicate this requirement contributed to the breach. Their justification is below:
>
> **Services allowing remote access (RDP) into the cardholder data environment from untrusted networks facilitated the attacker in compromising cardholder data.**
>
> - Visa does not agree with TW's assessment that Genesco is in violation of Req 1. RDP was running on the internal network. TW should have reviewed to determine if a firewall exists between the corporate WAN and the payment card data environment (although this does not appear to be a PCI requirement, either). Per PCI DSS v2.0, Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is **not** a PCI DSS requirement. However, it is strongly recommended. PCI DSS does require that, if there is no segmentation, the entire network is in scope of the PCI DSS assessment. Question for Genesco, did their previous PCI assessment included the entire network?
>
> - Visa does agree that RDP contributed to the breach. Questions for TW: 1) **Per PCI DSS requirement 2.3, all non-console administrative access must be encrypted. Did Genesco used VPN/SSH/SSL/TLS to encrypt RDP sessions? If not, Genesco was in violation of 2.3. This should have been documented on the forensic report and reflected on the PCI DSS Requirements Overview.**
>
> **Requirement 8 - Assign a unique ID to each person with computer access**

Trustwave findings indicate this requirement contributed to the breach. Their justification is below:

The third-party support account was enabled at all times. VPN access into the cardholder data environment wasn't enforcing two-factor authentication.

Visa's review of forensic findings:

- Visa agrees with TW's assessment that Genesco is in violation of Req 8. Per forensic report, pages 15 and 32, remote access solution for third-party vendor accounts was persistently enabled, remote access for third-party accounts should be only accessible only on as as-needed basis and enforce two-factor authentication. Since Genesco did not have full segmentation (see network diagram on page 9), their corporate WAN would be in scope with PCI DSS and PFI forensic investigation. Thus, the following requirement would apply:

  - **8.5.6** Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.

  - In addition, Genesco was also in violation of **8.5.8** - Do not use group, shared, or generic accounts and passwords, or other authentication methods.

If Genesco disagrees, they must provide proof that their corporate WAN was completely segmented from the payment processing environment at the time of the security breach. This must be confirmed by TW since they performed the forensic investigation.

Requirement 11 - Regularly test security systems and processes.

Trustwave findings indicate this requirement contributed to the breach. Their justification is below:

The file integrity monitoring solution wasn't configured to monitor all critical system directories.

Visa's review of forensic findings:

- Visa agrees with TW's assessment that Genesco was in violation of Req 11. Per forensic report page 33, File integrity monitoring (FIM) software was not configured to monitor the Windows System32 directory. PCI DSS req 11 requires the following:

- o Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

- System32 is a directory which contains critical system files (i.e., executables, DLLs, etc.). This is a standard directory where critical system files are installed. FIM should have been monitoring the system32 directory within the payment card switch servers. Furthermore, it is a PCI requirement to alert personnel in the event of modification to critical system files.

(Docket Entry No. 106 at 1-2) (emphasis added in part). On November 7, 2011, Visa voted to qualify the Intrusion for its ADCR and DCRS programs based only on the "Qualification Summaries" that Visa staff had prepared. (Docket Entry No. 164 and 224 at 2).

Between November 7, 2011 and January, 2013, Fifth Third and Wells Fargo had discussions with Visa on Visa's qualification process. Visa extended the appeal deadline during these discussions. (Docket Entry Nos.159, 161, 162, 168, 173 and 175). On November 22, 2011, Fifth Third and Wells Fargo requested information and on January 9, 2012, Visa responded to some, but not all of the November 22nd requests. (Docket Entry Nos.159, 161, 167, 168). The Banks and Visa negotiated production of the unanswered requests. (Docket Entry No. 151, Harrington Affidavit at ¶ 71). During this time period, the Banks' appeal was stayed, and Genesco provided additional information and documentation to Visa and sought reciprocity from Visa. (Docket Entry Nos.169-170). During this time period, Visa did not request any information about Genesco's PCI DSS compliance or non-compliance[3], but sought information about Genesco's assertions that reboots of Genesco's servers caused the overriding of the Intruder-created log files. (Docket Entry No. 169). Ultimately, Visa did not request any additional information about Genesco's PCI DSS compliance

[3]According to Genesco, Visa considered the information and documentation requested by Genesco in the period after issuing the Qualification Summaries "not germane" (Docket Entry Nos.167-169) .

or non-compliance. (Docket Entry No. 151, Harrington Affidavit at ¶ 71).[4]

At some undefined point "late 2012", Visa purportedly declined any more extensions of the Banks' appeal. (Docket Entry No. 227 at 4). On September 28, 2012, Visa stated that "based on the information in the January 27, 2011 Trustwave Forensic Report, the identification of affected accounts provided by Genesco's acquirers, and the overall counterfeit fraud experienced by the accounts included in the qualification . . . Visa continues to believe that the Genesco account data compromise event was properly qualified" under the ADCR and DCRS programs. (Docket Entry No. 151, Harrington Affidavit at ¶ 74). On October 26, 2012, Genesco and the Acquiring Banks decided not to pursue the appeal, given Visa's refusal to provide the information sought by their November 22 requests and because they considered the VIOR appeal process to be presumptively biased in Visa's favor. (Docket Entry No. 67, Rofkar Affidavit, at ¶¶ 16-17 and Docket Entry No. 54 at 7 n.1).

2. Visa's Relevant VIOR

Visa's VIOR sets forth the governing principles for Visa's assessments of fines and reimbursements against Acquiring and Issuing Banks that provide, in pertinent part:

> **Cardholder and Transaction Information Security- U.S. Region**
>
> **A U.S. Member must comply, and ensure that its Merchants and Agents comply, with the requirements of the Cardholder Information Security Program, available from Visa upon request or online at http://www.visa.com/cisp.**
>
> A third party that supports a loyalty program or provides fraud control services, as specified in "Disclosure of Visa Transaction Information- U.S. Region" and "Cardholder and Transaction Information Disclosure Limitations - U.S. Region," must comply with the requirements of the Cardholder Information Security Program.

---

[4] In this connection, Visa quoted a statement that, in essence, Visa considers various sources of information, (Docket Entry No. 210 at 5), but the cited Docket Entry does not contain the Exhibit Z quoted by Visa. The Court also is concerned that the Beierly memorandum, a significant three page document, is lacking the third page.

A **U.S. Member must comply, and ensure that its Merchants and Agents comply, with the Transaction Information security requirements in the Visa *International Operating Regulations*, the Payment Card Industry Data Security Standard (PCI DSS), and the validation and reporting requirements outlined in the Cardholder Information Security Program. The Payment Card Industry Data Security Standard (PCI DSS) and the Cardholder Information Security Program requirements are available online at http://www.visa.com/cisp.**

An Acquirer must ensure that its Merchant:

- Implements and maintains all of the security requirements, as specified in the Cardholder Information Security Program
- Immediately notifies Visa, through its Acquirer, of the use of a Third Party
- Ensures that the Third Party implements and maintains all of the security requirements, as specified in the Cardholder Information Security Program
- Immediately notifies Visa, through its Acquirer, of any suspected or confirmed loss or theft of material or records that contain account information and:

- Demonstrates its ability to prevent future loss or theft of account or Transaction information, consistent with the requirements of the Cardholder Information Security Program

- Allows Visa, or an independent third party acceptable to Visa, to verify this ability by conducting a security review, at the Acquirer's own expense

ID#: 010410-010410-0008031

Fines and Penalties

Non-Compliance with Account and Transaction Information Security Standards VIOR 2.1.E

If Visa determines that a Member, its agent, or a Merchant has been deficient or negligent in securely maintaining the account or Transaction Information or reporting or investigating the loss of this information, Visa may fine the Member, as specified in the Visa *International Operating Regulations*, or require the Member to take immediate corrective action.

ID#: 010410-010410-0001753

Issuer Identification on Card

Visa identifies the Issuer that ordered the manufacture of a Visa Card or Visa Electron Card by either the name printed on the Visa Card or Visa Electron Card or the manufacturer product information printed on the back of the Visa Card or Visa Electron Card.

There is no time limit on a Member's right to reassign liability to the Issuer under this section.

ID#: 010410-010410-0008158

Counterfeit Card Transaction Reporting

If a Member discovers Counterfeit Card activity, the Member must immediately report the Account Number to Visa.

ID#: 010410-010410-0001816

Account Data Compromise Recovery (ADCR)

Account Data Compromise Recovery Process - U.S. Region

In the U.S. Region, the Account Data Compromise Recovery (ADCR) process allows Visa to determine the monetary scope of an account compromise event, collect from the responsible Member, and reimburse Members that have incurred losses as a result of the event.

ADCR allows the recovery of counterfeit transaction losses across all Visa-owned brands (i.e., Visa, Interlink, and Plus) when a violation attributed to another Visa Member could have allowed data to be compromised and the subsequent financial loss was associated with any of the following:

- A Visa Transaction
- An Interlink transaction
- A Plus transaction

This process is only available when there has been a violation of at least one of the following:

- Operating Regulations involving electronic storage of the full contents of any track on the Magnetic Stripe subsequent to Authorization of a Transaction

- Operating Regulations involving non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of the full contents of any track on the Magnetic Stripe

- Operating Regulations involving the PIN Management Requirements Documents that could allow a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization

The Account Data Compromise Recovery process includes:

- Counterfeit Fraud Recovery

- Operating Expense Recovery

ID#: 081010-010410-0000877

Transactions Excluded from ADCR Process - U.S. Region

In the U.S. Region, violations of the Visa *International Operating Regulations* not involving storage of Magnetic-Stripe Data are excluded from this process.

In the U.S. Region, violations not involving non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of the full contents of any track on the Magnetic Stripe are excluded from this process.

Violations not involving a Transaction are resolved as specified in "Visa Right to Fine" and as deemed appropriate by Visa.

ID#: 081010-010410-0000878

Determination of ADCR Eligibility -U.S. Region

Effective for Qualifying CAMS Events that occurred on or before 30 March 2009, following the fraud analysis and investigation of the compromise event, a U.S. Member:

- Is provided with findings in support of the preliminary determination that the event is eligible for the ADCR process

- Is provided with any estimated counterfeit fraud and operating expense

liability amounts

- May submit a written appeal, within 30 calendar days of the preliminary findings notification date, with supporting documentation to Visa. Such appeal will be considered by the ADCR Review Committee or, if the total Acquirer liabilities are US $500,000 or more, the appeal will be considered by the Corporate Risk Committee. A determination of such appeal will be provided to the Acquirer.

Effective for Qualifying CAMS Events that occur on or after 31 March 2009, following the fraud analysis and investigation of the compromise event, the U.S. Member is provided with:

- Findings in support of the preliminary determination that the event is eligible for the ADCR process
- Any estimated counterfeit fraud and operating expense liability amounts

ID#: 010410-010410-0009035

Counterfeit Fraud Recovery Process -U.S. Region

A U.S. Member is compensated for a portion of its counterfeit fraud losses incurred as the result of a Magnetic-Stripe Data account compromise event. The Counterfeit Fraud Recovery process is initiated by Visa when:

- An account compromise event occurs
- A Compromised Account Management System (CAMS) Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members
- Effective for Qualifying CAMS Events that occur on or before 30 June 2010, the account compromise event involves at least 10,000 Account Numbers
- **Effective for Qualifying CAMS Events that occur on or after 1 July 2010,** the account compromise event involves at least 10,000 Account Numbers **and** a combined total of US $100,000 or more recovery for all Issuers involved in the event

- At least one of the following:

  - The full contents of any track on the Magnetic Stripe was stored subsequent to Authorization of a Transaction

- A violation of the Payment Card Industry Data Security Standard (PCI DSS) could have allowed a compromise of the full contents of any track on the Magnetic Stripe

- A violation of the PIN Management Requirements Documents could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization

- Incremental fraud is attributed to the particular account compromise event

ID#: 081010-010410-0000880

Counterfeit Fraud Reimbursement Conditions - U.S. Region

In the U.S. Region, only counterfeit fraud properly reported as specified in the *Visa International Operating Regulations* is considered when determining any reimbursement due.

ID#: 010410-010410-0000881

Baseline Counterfeit Fraud Level Determination- U.S. Region

In the U.S. Region, Visa determines a baseline counterfeit fraud level by analyzing reported Magnetic-Stripe-read counterfeit fraud losses that occurred up to 12 months before a Qualifying CAMS Event date and one month after the Qualifying CAMS Event date.

ID#: 010410-010410-0000882

Counterfeit Fraud Recovery Eligibility- U.S. Region

U.S. Members are eligible for Counterfeit Fraud Recovery when there is incremental counterfeit fraud activity above the baseline counterfeit fraud level, as determined by Visa.

ID#: 010410-010410-0000883

Counterfeit Card Recovery Process - U.S. Region

The U.S. Member deemed responsible for an account compromise event is notified of its estimated counterfeit fraud liability.

After the deadline for fraud reporting has passed, a Member communication broadcast is

used to notify affected U.S. Members that an account compromise event qualifies for Counterfeit Fraud Recovery and advises them of their recovery amount.

The U.S. Member deemed responsible for the account compromise event is then notified of its actual counterfeit fraud liability.

ID#: 010410-010410-0008117

ADCR Reimbursement Guidelines- U.S. Region

The following rules are related to the recovery process in the U.S. Region:

- Only recovery amounts of US $25 or more are collected and distributed to affected U.S. Members.
- Only U.S. Members that were registered to receive CAMS Alerts at the time of the first CAMS Alert for the event that is the subject of the ADCR proceeding are eligible to receive counterfeit fraud reimbursement.
- Counterfeit fraud losses on Account Numbers that were included in a different Qualifying CAMS Event within the 12 months before the Qualifying CAMS Event date are excluded.
- If 2 or more Qualifying CAMS Events occur within 30 days of each other, and the events each involve a minimum of 100,000 Account Numbers, the responsible U.S. Members share liability for the counterfeit fraud amount attributed to the accounts in common.

ID#: 010410-010410-0000887

Counterfeit Fraud Liability Collection and Distribution -U.S. Region

Counterfeit fraud liability is collected from the responsible U.S. Member(s) through the Global Member Billing Solution. Funds are distributed the following month, at the Business 10 level, through the Global Member Billing Solution, to affected Members.

ID#: 010410-010410-0000888

ADCR Administrative Fees - U.S. Region

In the U.S. Region, an administrative fee is charged to the Issuer for each reimbursement

issued, as specified in the *Visa U.S.A. Fee Guide*.

ID#: 081010-010410-0000889

Operating Expense Recovery Process -U.S. Region

A U.S. Member enrolled in the Operating Expense Recovery process is compensated for a portion of its operating expenses incurred as a result of a Magnetic-Stripe Data account compromise event. The Operating Expense Recovery process is initiated by Visa when:

- An account compromise event occurs
- A CAMS Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members
- Effective for Qualifying CAMS Events that occur on or before 30 June 2010, the account compromise event involves at least 10,000 Account Numbers
- **Effective for Qualifying CAMS Events that occur on or after 1 July 2010**, the account compromise event involves at least 10,000 Account Numbers and a combined total of US $100,000 or more recovery for all Issuers involved in the event

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, in the U.S. Region, the appeal rights, as specified in "Enforcement Appeals- U.S. Region," are **not** applicable to ADCR.

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, Visa will notify the U.S. Member of the final disposition of the appeal.

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, in the U.S. Region, the decision on any appeal is final and not subject to any challenge.

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, Visa will collect from the U.S. Member an appeal fee, as specified in the *Visa U.S.A. Fee Guide*, through the Global Member Billing Solution. For a data compromise event that qualifies under both the ADCR process and the international Data Compromise Recovery solution, Visa will collect only one appeal fee from the Member, as specified in the *Visa U.S.A Fee Guide.*

ID#: 081010-010410-0009036

Data Compromise Recovery Solution (DCRS)

Data Compromise Recovery Solution Overview

An Issuer of Visa International or Visa Europe may recover incremental counterfeit fraud losses resulting from a Data Compromise event involving theft of full Magnetic-Stripe Data under the Data Compromise Recovery solution from Member(s) to whom liability for such loss has been assigned pursuant to the Data Compromise Recovery solution.

ID#: 010410-010410-0003334

Data Compromise Recovery Solution Eligibility

Visa will determine a data compromise event, fraud, and Issuer eligibility under the Data Compromise Recovery Solution.

ID#: 010410-010410-0003335

Data Compromise Event Eligibility

Visa will determine data compromise event eligibility based on:

- **Forensic confirmation or preponderance of evidence that a breach exists**
- **A violation of the Payment Card Industry Data Security Standard (PCI DSS) occurred that could allow a compromise of account data**
- **Full Magnetic Stripe counterfeit fraud occurred on a portion of exposed Account Numbers**
- **A minimum of 10,000 Account Numbers were exposed and a minimum of US $100,000 in Magnetic Stripe counterfeit fraud occurred during the data compromise event time period**

ID#: 010410-010410-0000867

Data Compromise Fraud Eligibility Criteria

Visa will determine fraud eligibility based on all of the following:

- **Counterfeit fraud was reported to Visa**

- **Authorized counterfeit fraud Transactions with full Magnetic-Stripe Data occurred, including Card Verification Value**

- **Counterfeit fraud Transactions occurred after the Magnetic-Stripe Data was exposed**

ID#: 010410-010410-0000868

Unrecovered Counterfeit Fraud Losses

Visa will determine Issuer eligibility for unrecovered counterfeit fraud losses, based on the Issuer being:

- Capable of receiving Visa data compromise fraud alerts

- In compliance with regional Issuer fraud control programs

ID#: 010410-010410-0000869

Data Compromise Recovery Liability Time Limit

An Acquirer's liability under the Data Compromise Recovery solution is limited to a maximum time period of 13 months and is associated with a single data compromise event.

ID#: 010410-01041 0-0000870

Data Compromise Event Time Period

The data compromise event time period begins with the earliest known data exposure, not to exceed 12 months before the data compromise event alert and concludes 30 calendar days following the data compromise event alert.

ID#: 010410-010410-0000871

Data Compromise Fraud Loss Recovery

Issuers' total fraud loss recovery is limited to the:

- Maximum liability assigned to the Acquirer by Visa

- Amount recoverable from the Acquirer

ID#: 010410-010410-0000872

(Docket Entry No. 135-1 at 3-9) (emphasis added to text).

3. Genesco's Retention of the Stroz Firm

Earlier, on December 3, 2010, Roger Sisson, Genesco's general counsel, engaged the Stroz Friedberg firm ("Stroz") to provide consulting and technical services to assist Sisson and Genesco's outside counsel in rendering legal advice to Genesco about the Intrusion and Trustwave's report. (Docket Entry No. 91, Sisson Affidavit at ¶12 and Docket Entry No. 92, Meal Affidavit at ¶7). According to Sisson, the process and organization for Genesco's response to Trustwave's report were as follows:

> 5. Genesco did not conduct an investigation of its own regarding the possibility of a compromise of Genesco's network prior to Trustwave's arrival onsite on November 30, 2010.
>
> 6. Genesco cooperated fully with Visa's investigation of the Intrusion and Trustwave's forensic evaluation of Genesco's network. Genesco provided Trustwave with access to all information and material requested by Trustwave in connection with the Intrusion.
>
> 7. On November 30, 2010, Trustwave advised Genesco that it had detected suspicious software on Genesco's network and that it had concluded, based on this finding, that Genesco had suffered an intrusion (the "Intrusion") into the portion of its computer system that processes and stores information regarding credit and debit card transactions made at its stores.
>
> 8. On that same day, I had a conversation with Henry Walker ("Walker"), litigation partner at Kilpatrick Townsend & Stockton LLP, regarding Trustwave's findings and the potential legal ramifications and his experience with prior data breaches, including the likelihood of litigation, and, on behalf of Genesco, I retained Kilpatrick Townsend & Stockton LLP to render legal advice to Genesco in connection with the Intrusion.
>
> 9. On December 2, 2010, I had a conversation with Douglas Meal ("Meal"), litigation partner at Ropes & Gray, regarding Trustwave's findings and the potential legal ramifications of a computer systems intrusion, including the likelihood of litigation, in particular litigation arising out of claims by the payment card brands such as Visa, and on

behalf of Genesco, I retained Ropes & Gray to render legal advice to Genesco in connection with the Intrusion.

10. Following consultation with Walker, Meal and myself (jointly, "Genesco Counsel"), Genesco determined that Genesco Counsel should conduct an investigation of the Intrusion, separate and apart from the investigation already being conducted by Trustwave on behalf of Visa and the other major card brands, for the purpose of providing legal advice to Genesco regarding the Intrusion and in anticipation of litigation with the card brands and other persons arising out of the Intrusion (the "Privileged Investigation").

11. On the next day, Genesco Counsel identified the need to retain a computer security consultant to assist them in conducting the Privileged Investigation. Meal selected Stroz Friedberg LLC ("Stroz Friedberg") to be the retained consultant, based on previous engagements.

12. On December 3, 2010, I, as General Counsel on behalf of Genesco, retained Stroz Friedberg to provide consulting and technical services at the direction of Genesco Counsel to assist Genesco Counsel in rendering legal advice to Genesco in anticipation of litigation and/or other legal or regulatory proceedings.

13. Attached as Exhibit 1 submitted under seal pursuant to a Motion to Seal filed with the Court on October 16, 2013, is the engagement letter with Stroz Friedberg dated December 3, 2010.

14. Genesco Counsel, with the assistance of Stroz Friedberg, conducted the Privileged Investigation. Any and all investigation, analysis, and reviews performed in the course of the Privileged Investigation were done to assist Genesco Counsel in preparing for anticipated litigation with the card brands and other persons arising from the Intrusion and in providing legal advice to Genesco relating to the Intrusion. Genesco did not conduct any investigation of the Intrusion separate and apart from the Privileged Investigation.

15. Any and all contacts, correspondence, meetings or other interactions between Genesco and Stroz Friedberg concerning the Intrusion occurred either with or at the direction of Genesco Counsel.

(Docket Entry No. 91).

The Genesco-Stroz retention agreement expressly provided that Stroz's retention was "in anticipation of potential litigation and/or legal or regulatory proceedings." (Docket Entry No. 116, Sisson Affidavit, Exhibit No. 1 thereto at 1-2). Genesco is not presenting the Stroz's consultant or the Stroz report that Genesco disclosed to Visa prior to this litigation, as evidence for its claims in

this action.

B. The Disputed Discovery Requests and Discovery Issues

For these motions, Visa's specific discovery requests seek documents and an answer to one interrogatory that are worded as follows:

> REQUEST FOR PRODUCTION No. 11: All DOCUMENTS relating to YOUR compliance or non-compliance with the CARDHOLDER ACCOUNT DATA SECURITY REQUIREMENTS, including without limitation any and all internal reports and external COMMUNICATIONS, for the time period from January 1, 2007 to present.
>
> REQUEST FOR PRODUCTION No. 12: All COMMUNICATIONS relating to YOUR compliance or non-compliance with the CARDHOLDER ACCOUNT DATA SECURITY REQUIREMENTS, including without limitation any and all internal and external COMMUNICATIONS, for the time period from January 1, 2007 to present.
>
> REQUEST FOR PRODUCTION No. 15: All DOCUMENTS related to the INTRUSION, including but not limited to any investigation by YOU (or on YOUR behalf) relating to the INTRUSION or any COMMUNICATIONS by YOU relating to the INTRUSION.
>
> REQUEST FOR PRODUCTION No. 16: All DOCUMENTS related to the PERSON(S) that provided YOU with any component or services in connection with the GENESCO PAYMENT PROCESSING NETWORK in use during the INTRUSION through the present time.
>
> REQUEST FOR PRODUCTION No. 17: All COMMUNICATIONS involving YOU and any third party discussing or referencing forensic information or any investigation related to the INTRUSION.
>
> REQUEST FOR PRODUCTION No. 30: All COMMUNICATIONS related to the INTRUSION, including but not limited to any investigation by YOU (or on YOUR behalf) relating to the INTRUSION.
>
> REQUEST FOR PRODUCTION No. 31: All COMMUNICATIONS between YOU and the PERSON(S) that provided YOU with any component or any service in connection with the GENESCO PAYMENT PROCESSING NETWORK in use during the INTRUSION through the present time
>
> Visa's INTERROGATORY: Identify everything Genesco did to change, modify or alter in any way its corporate wide area network (WAN) computer system or its CARDHOLDER DATA ENVIRONMENT computer system after the INTRUSION, and state all facts as to why such changes were made

(Docket Entry No. 120, Visa's Motion to Compel at 2, 5, 6, 8, 9, 10, 11 and 13 and Docket Entry No. 133, Visa's Motion to Compel at 5, 6, 8, 9, and 13). These motions involve the same requests and interrogatory.

Visa also issued a subpoena to Stroz for documents and deposition testimony on Stroz's "relationship with Genesco" Stroz's "investigation, analysis, and review of any kind whatsoever related to the Intrusion" and the results of any such "investigation, analysis, or review"; Stroz's "contacts, correspondence, meetings, and other interactions with Genesco or third parties concerning the Intrusion;" Stroz's Incident Reboot Analysis of Genesco's network and compliance or non-compliance with the PCI DSS during the period January 1, 2009 through the present and "any post-Intrusion remediation or enhancements" to Genesco's network, Stroz's "review and evaluation, if any, of the Trustwave's Incident Response Final Report Addendum," and Stroz's "involvement or assistance with, or input or contribution to, the annotated report." (Docket Entry No. 203-1, Notice of Subpoena at 8-9). Additionally, the Stroz subpoena seeks production of "all communications and documents" on the same topics. Id. at 13-15. Visa later noticed Sisson, Genesco's general counsel, for a deposition on the same subjects. (Docket Entry No. 237-1).

According to the parties' discovery motions, their current discovery issues involve the following topics:

- discovery of Genesco's investigation, analysis and reviews into the Intrusion, including its interactions with third parties, such as the Stroz firm (Topic Nos. 7, 9, 24);
- discovery of Genesco's knowledge, understanding, and conduct in connection with **all** PCI DSS requirements and its compliance with those requirements (Topics 19 and 20);
- Discovery of Genesco's submission of various assessments and reports on such compliance or non-compliance to Wells Fargo and Fifth Third (Topic Nos. 10, 15,

21, 22, 23, 25);

- discovery of Genesco's computer system, including those aspects of Genesco's system specifically analyzed or discussed by Trustwave, which Genesco retained to investigate the Intrusion, both before and after the Intrusion (Topic Nos. 18, 19, 20).

(Docket Entry No. 88-1, Parties' Joint Discovery Statement)

- Whether Genesco must conduct "a reasonable non-ESI search for and produc[e] [to the extent located by means of such search] (1) any document reflecting Genesco's PCI DSS compliance policies, including analyses, meeting minutes, or other reasonably identifiable documents discussing those policies and (2) any documents discussing Genesco's actual or potential non-compliance with the PCI DSS and any other applicable cardholder account security requirements during the period of the Intrusion" and (B) to conduct an additional ESI-based search for documents responsive to such requests generated prior to Genesco's retention of outside counsel in connection with the Intrusion on November 30, 2010" to respond to Visa's Document Request Nos. 11-2, 15-17 and 30-31

(Docket Entry No. 139, Parties' Joint Discovery Statement)

- Whether the Stroz firm is a fact witness subject to discovery or a non-testifying consultant expert under Rule 26(b)(4)(D) for which there is not any showing of exceptional circumstances

(Docket Entry No. 201-2, Parties' Joint Discovery Statement)

In summary, the parties' Topic No. 7 seeks discovery including the Stroz firm as Visa is requesting "Genesco's investigation, analysis and reviews of any kind in relation to the Intrusion, including **but not limited to those performed** internally or **through vendors and service providers**, and all other Communications and Documents with respect thereto." (Docket Entry No. 90-1, Exhibit A to Harrington Affidavit at 8). (emphasis added). Topic No. 9 also seeks discovery of "GENESCO's contacts, correspondence, meetings, and other interactions with Stroz Friedberg" connected to Trustwave's investigation of the Intrusion and Trustwave's Incident Response Report. Id. at 8-9. Topic Nos. 19, 20, and 25 seek information regarding Genesco's post-Intrusion

remediation of its security system to prove that Genesco's assertions regarding its compliance with all PCI DSS requirements prior to and during the Intrusion are unfounded. Id. at 11-12. Topic No. 22 also involves testimony about Genesco's submission of a Completed Self-Assessment Questionnaire to Wells Fargo and Fifth Third. Id. at 12.

1. Genesco's Objections

For these discovery issues, Genesco raises three core objections, namely that Visa's discovery requests are irrelevant, unduly burdensome, and seek privileged information:

- the irrelevancy objection involves communications on Genesco's data-security systems in place on Genesco's computer networks and Genesco's knowledge of and compliance or non-compliance with all applicable cardholder security requirements other than the PCI DSS violations found by Trustwave;

- another irrelevancy objection is to documents related to and communications with the persons or entities that provided Genesco with services related to its payment processing network; and

- the privilege objections are to Genesco's internal documents and communications regarding the Intrusion by Genesco's counsel and its consultant, the Stroz firm

As to Topics 7, 9, and 24, Genesco asserts that its investigation was conducted by Genesco's counsel with expert assistance in anticipation of litigation. (Docket Entry No. 92, Meal Affidavit at ¶8). As a result, Genesco contends that all the testimony sought by Topic No. 7 falls squarely within Rule 26(b)(4)(D). Genesco's burdensomeness objection on Topic 9, in pertinent part, is as follows:

> Trustwave already conducted on Visa's behalf, and Genesco fully complied with, a full investigation of Genesco's compliance or non-compliance with the Cardholder Account Data Security Requirements at the time of the Intrusion, during which investigation **Genesco made available to Trustwave all documents Trustwave deemed necessary to conduct such investigation . . . and based on which investigation Visa concluded it had sufficient information to impose the unlawful assessments that are the subject of this action.**

(Docket Entry No. 136-1, Carrillo Affidavit Exhibit N thereto at 11) (emphasis added).

As to Topic Nos. 19, 20, and 25 Genesco reasserts its relevancy and privilege objections on Genesco's post-Intrusion remediation of its security system and argues that Topic Nos. 22 and 24 on Genesco's assessments and communications with third parties related to the Intrusion or vulnerabilities related to the Intrusion are irrelevant. (Docket Entry No. 136-1,Carrillo Affidavit, Exhibit N thereto).

Genesco characterizes the material sought by the Sisson deposition notice and the Stroz subpoena as privileged under the attorney client and work product privileges and barred by Fed. R. Civ. P. 26(b)(4)(D) absent a showing of extraordinary circumstances, that Visa has not made. Notwithstanding its objections, Genesco agreed to produce a Rule 30(b)(6) deponent to testify on the following subjects listed in Visa's Rule 30(b)(6) Notice:

(1) the four PCI DSS requirements that Visa considered in determining to impose and collect the Fines and Assessments;
(2) the specifics of Genesco's contention that Trustwave incorrectly concluded that these four PCI DSS requirements were not "in place" at the time of the Intrusion; and
(3) the four PCI DSS requirements that Visa considered in imposing the Fines and Assessments

Genesco produced Sisson as a Rule 30(b)(6) witness on the subject of Genesco's obligations to Fifth Third and Wells Fargo.

2. Visa's Responses

As to the relevancy objections, Visa cites the following allegations in Genesco's complaint as justifying discovery related to Genesco's compliance with all PCI DSS requirements:

- "[A]t the time of the Intrusion and at all other relevant times Genesco was in compliance with the PCI DSS requirements." (Docket Entry No. 1, Complaint at ¶ 48.)

- "Visa could not possibly have had a valid basis under the VIOR for imposing the Non-Compliance Fines, even if Fifth Third and/or Wells Fargo had at some relevant time violated its contractual obligations to Visa to cause

Genesco to maintain compliance with the PCI DSS requirements (which neither of them did)." Id. at ¶ 50.

- "Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco committed a PCI DSS violation that allowed the theft of cardholder data . . . ." Id. at ¶¶ 55, 61, 67.

(Docket Entry No. 184 at 9-10, 11). The Court construed these references to refer to the VIOR rules that were the bases for the Visa's fines and assessments that Genesco sought to recover.

At oral argument and in supplemental memoranda, Visa's counsel cited other relevant paragraphs of Genesco's complaint, but none contained Visa's counsel's characterization of those paragraphs' allegations. Based upon Visa's counsel's argument, the Court conducted a word search of Genesco's complaint for any allegation of Genesco's compliance with "all" Visa rules or "full" compliance with Visa rules or "complete" compliance with Visa rules. Such allegations were not found in Genesco's complaint. Visa contends that these three allegations and similar allegations in Genesco's complaint place all of Genesco's computer payment network at issue for discovery. Visa further contends that any non-compliance by Genesco with any CISP or PCI DSS requirement could justify Visa's fines and assessments. Visa notes that Genesco propounded a separate set of interrogatories seeking information about Visa's Cardholder Information Security Program ("CISP").

As to the privilege assertions, Visa cites Genesco's providing Visa with two documents from Genesco's counsel's investigation and a report from Genesco's consultant as constituting waivers of the privileges asserted for discovery and that these waivers extend to Genesco's computer expert's communications with Genesco's counsel during Genesco's internal investigation. (Docket Entry No. 184 at 24-25). Moreover, Visa cites Genesco's failure to file privilege logs, as required by precedents of this Court to assert these privileges, as a waiver of these privileges. Visa also characterizes its discovery of the Stroz firm as fact discovery. Finally, Visa argues that Genesco's

objections based upon Fed. R. Evid. 407 are misplaced and cites authorities that Rule 407 is inapplicable during discovery. Visa also requested Genesco to provide contrary authority or amend its responses to the Requests, but Genesco did not do so.

C. Conclusions of Law

1. The Relevancy Objections

Federal Rule of Civil Procedure 26 permits parties to "obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party. . . . Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." Fed. R. Civ. P. 26(b)(1). Under Rule 26(b)(1), "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense...." Given Rule 26(b)(1)'s clear focus on relevance, "[a] district court does not abuse its discretion in denying discovery when the discovery requested would be irrelevant to the underlying issue to be decided." Sigmon v. Appalachian Coal Properties, Inc., 400 Fed. Appx. 43, 51 (6th Cir. 2010) (quoting Green v. Nevers, 196 F.3d 627, 632 (6th Cir. 1999) and citing Elvis Presley Enters. v. Elvisly Yours, Inc., 936 F.2d 889, 894 (6th Cir.1991) ("The District Court did not abuse its discretion in limiting discovery on this issue, which is not relevant in this case.").

Under federal discovery rules, for a breach of contract action, discovery is "[g]enerally... relevant if it seeks information pertinent to allegations in the pleadings" and "documents in the defendant's control relating to the third party's refusal to accept the product" or "to the specific complaint they have alleged in their pleadings" Moore's Federal Prac. Vol. 6, §26.46[4] at 26-238, 26-241 (3d ed.). In the decisions cited in Moore's, the defendants sold multiple brands or models, but only the brand or model giving rise to the claims was ruled appropriate for discovery. Id. citing

Camden Iron & Metal Inc. v. Marubeni Am. Corp., 138 F. R. D. 438, 441 (D. N. J. 1991); Schaap v. Executive Indus. Inc, 130 F. R. D. 384, 289 (N. D. Ill. 1990): Detweiler Bros. Inc. v. Inc. v. John Graham & Co., 412 F. Supp. 416, 422 (E. D. Wash. 1976); Blatt v. Cass Blanca Cigar Co., 51 F. R. D. 312, 313 (M. D. Pa. 1970).

Visa contends that the language of the pleadings controls the scope of discovery, but that contention ignores the plain language of Rule 26(b)(1) that "[r]elevant information need not be admissible at the trial **if the discovery appears reasonably calculated to lead to the discovery of admissible evidence**." (emphasis added). As stated in Grant, Konvalinka & Harrison, P.C. v. United States, No. 1:07–CV–88, 2008 WL 4865566 at *4 (E.D.Tenn.,2008 Nov.10, 2008) "a party seeking the discovery still has the burden of proving that any settlement agreement sought must contain information relevant to the claim or defense of any party and, **must be either admissible at trial, or reasonably calculated to lead to the discovery of admissible evidence.**" (emphasis added) (citing Allen v. Howmedica Leibinger, Inc., 190 F.R.D. 518, 522 (W.D.Tenn.1999) (citing Andritz Sprout–Bauer v. Beazer East, 174 F.R.D. 609, 631 (M.D.Pa.1997)). The Court in Grant also cited Monsanto Co. v. Ralph, 2001 WL 35957201, 2001 U.S. Dist. LEXIS 26151 (W.D.Tenn. May 9, 2001) that "differentiating between instances when discovery sought appears relevant, in which case **the party resisting discovery bears the burden of establishing lack of relevance, and instances where the relevancy is not apparent, in which case the party seeking discovery bears the burden**" Id.(emphasis added). Thus, Rule 26(b) requires some consideration of the substantive law on Genesco's claim because Genesco's objection is that Visa's discovery could not lead to the discovery of admissible evidence. Genseco's specific relevancy objection is that Visa's discovery requests for all VIOR rules would not likely result in discovery of admissible evidence on the VIOR

rules that were the bases for the fines and assessments at issue. Thus, pleadings alone do not control the scope of appropriate discovery

Moreover, Visa's contention is contrary to the decisions cited in Moore's and the above cited precedents that limit discovery in breach of contract actions to the contract provisions giving rise to the breach. Here, Genesco is suing for recovery of fines and assessments based upon a report that Visa directed to be completed. Discovery of other parts of Genesco's computer system that were not the bases for the fines and assessments would not lead to discovery of relevant information about the bases for Visa's fines and assessments. As Visa stated in its theory of the case: **"Visa applied the applicable VIOR rules** and determined that Genesco's two Acquiring Banks -- Wells Fargo and Fifth Third were required to make payments totalling $13,288,900". (Docket Entry No. 25, Case Management Order at 4) (emphasis added). If there are other closely related VIOR rules that Genesco is alleged to have violated and were relied upon for Visa's fines and assessments, then Visa can frame more targeted discovery requests.

For this breach of contract action, Genesco bears the burden to prove: (1) the existence of a valid contract; (2) that Visa breached that contract; and (3) that Visa's breach caused Genesco's damage, citing Troyk v. Farmers Grp., Inc., 171 Cal. App. 4th 1305, 1352–53 (2009). According to Visa, the causation element requires proof that the breach was "a substantial factor in causing the damages," Id. (quoting US Ecology Inc. v. State, 129 Cal. App. 4th 887, 910 (2005)).

Genesco contends that the "mend the hold" doctrine under California law operates to limit discovery to the specific bases upon which Visa relied for its assessments and fines. The "mend the hold" doctrine applies "where a party gives a reason for his conduct and decision touching any thing involved in a controversy, he cannot, after litigation has begun, change his ground, and put his

conduct upon another and a different consideration. He is not permitted to mend his hold" . Harbor Ins. Co. v. Continental Bank Corp., 922 F.2d 357, 364 (7th Cir. 1990) (quoting Railway Co. v. McCarthy, 96 U. S. 258, 267-68 (1877) "The phrase 'mend the hold' comes from nineteenth century wrestling parlance where it meant 'get a better grip (hold) on your opponent'." Robert H. Sitkoff, "MEND THE HOLD" AND ERIE: WHY AN OBSCURE CONTRACTS DOCTRINE SHOULD CONTROL IN FEDERAL DIVERSITY CASES", 65 U. Chi. L. Rev. 1059, 1060 (1998).

Since judicial recognition of the "mend the hold" doctrine, States differ in its application. "In its majority version, the mend the hold doctrine limits a nonperforming party's potential defenses for breaking a contract to those based on the prelitigation explanation for nonperformance that was given to the other party. In its minority form, mend the hold permits the changing of a contracting party's litigation posture only when that change comports with the implied duty of good faith that modern courts read into every contract." Id. (footnotes and internal quotations omitted). This doctrine is incorporated into the Uniform Commercial Code § 2-605.

To be sure, federal courts interpret the mend the hold doctrine in accordance with state law governing the parties' claims or defenses. Harbor Ins. Co., 922 F.2d at 362–63 (analyzing Illinois state law on mend the hold); Rupracht v. Certain Underwriters at Lloyd's of London Subscribing to Policy No. B0146LDUSA0701030, No. 3:11–CV–00654–LRH–VPC, 2012 WL 4472158 (D. Nev. Sept. 25, 2012) (Examining California law on "mend the hold" as substantive California law).

Genesco's claims are governed by California law and Genesco cites Alhambra Building & Loan Ass'n v. DeCelle, 47 Cal.App.2d 409, 411-12 (Cal. Ct. App. 1941) as recognizing this doctrine. There, a California appellate court observed in a title property dispute that the appellants "may not now 'mend their hold' or on appeal become self-appointed guardians of the rights of the

estate of the deceased" Id. at 411. In another decision, a California appellate court stated in an insurance contract controversy that "[t]here is nothing in this record to support the claim that the defendant suffered any injury of his rights by plaintiff's 'mending its hold'" John Hancock Mut. Ins. Co. v. Markowitz, 62 Cal. App.2d 388, 410, 144 P.2d 899 (1944). These California decisions that applied this doctrine in its rulings reflect California law's recognition of this doctrine in an appropriate case.

Visa contends that California law does not recognize the "mend your hold" doctrine citing Rupracht, 2012 WL 4472158 at *3 ("California—whose law governs here—has not adopted the mend the hold doctrine. Instead, California applies 'the general rule that waiver requires the insurer to intentionally relinquish its right to deny coverage and that a denial of coverage on one ground does not, absent clear and convincing evidence to suggest otherwise, impliedly waive grounds not stated in the denial.'") (quoting Waller v. Truck Insurance Exchange, Inc., 11 Cal.4th 1, 31-32 900 P.2d 619, 636 (1995)). Visa also cites Waller that involved a duty to defend under an insurance contract and discussed California's waiver doctrine, but does not include any references to the "mend your hold" doctrine. Neither Waller nor Rupracht cites nor discusses the two California appellate court opinions, Alhambra Building , 47 Cal.App.2d at 411 and Markowitz, 62 Cal. App.2d at 410, that expressly applied this doctrine to the facts in those cases. Second, the Rupracht decision cites to California's general contract law on waiver whereas the "mend your hold" doctrine is a distinct equitable doctrine. Third, a decision of a district court in another circuit is not binding on this Court. Generali v. D'Amico, 766 F.2d 485, 489 (11th Cir. 1985) (other circuit decisions not binding on Eleventh Circuit), but see Abex Corp. v. Maryland Cas. Co., 790 F.2d 119, 125-26 (D.C. Cir. 1986) (deference to out-of-circuit decision on question of state law within that circuit, absent a showing

of error). Because neither Rupratch nor Waller discusses or cites the California decisions recognizing the "mend the hold" doctrine, the Court respectfully declines deference to those decisions.

Moreover, the recovery of those fines and assessments by Genesco is tied to the violations of Visa's VOIR, CISP and PCI-DSS computer system requirements as found by Trustwave, for which Visa imposed its assessments and fines. These violations, if any, would be the substantial cause of the compromise in Visa's system and Visa's purported losses. Beyond general assertions and vague references to Genesco's allegations of compliance with VIOR rules, Visa has not shown nor can the Court discern how, discovery of other VIOR rules would impact the Banks and entities that were harmed by Genesco's alleged violations. Any violation of VIOR rules must be the substantial cause for Visa's fines and assessments. The Court also finds merit in Genesco's assertions that Visa's requests for discovery of its entire computer system lack any factual predicate as the PCI DSS requires quarterly checks of merchants for potential problems in Visa merchants' systems, citing "Validation procedures and documentation" published at *hhtp://usa.visa.com/merchants/risk_management/cisp_merchants.html*. Visa has not cited any other security violations by Genesco than those found by Trustwave.

As to Visa's contention that a VIOR violation "could" be the basis for its fines and assessment, the cited VIOR reads as follows:

Data Compromise Event Eligibility

Visa will determine data compromise event eligibility based on:

- **Forensic confirmation or preponderance of evidence that a breach exists**
- **A violation of the Payment Card Industry Data Security Standard (PCI DSS) occurred that could allow a compromise of account data**
- **Full Magnetic Stripe counterfeit fraud occurred on a portion of exposed**

Account Numbers

- **A minimum of 10,000 Account Numbers were exposed and a minimum of US $100,000 in Magnetic Stripe counterfeit fraud occurred during the data compromise event time period**

ID#: 010410-010410-0000867

Data Compromise Fraud Eligibility Criteria

Visa will determine fraud eligibility based on all of the following:

- Counterfeit fraud was reported to Visa
- Authorized counterfeit fraud Transactions with full Magnetic-Stripe Data occurred, including Card Verification Value
- Counterfeit fraud Transactions occurred after the Magnetic-Stripe Data was exposed

ID#: 010410-010410-0000868

(Docket Entry No. 135-1 at 8-9) (emphasis added). VIOR requires Visa to provide its "[f]indings in support of the preliminary determination that the event is eligible for the ADCR process," see (Docket Entry No. 135-1 at 5), "If there is no appeal for this case, Visa will process the settlement of this liability ... on January 15th, 2012." (Docket Entry Nos. 122-24).

While the term "could" is in this section of VIOR, the cardinal rule of contract construction is to consider other relevant portions of the contract that here includes the language requiring "[f]orensic confirmation or preponderance of evidence that a breach exists." (Docket Entry No. 135-1 at 8). Given Visa's own standard for fines and reimbursements, prior to any fine or assessment, Visa had to have proof of a VIOR violation. Visa also argues that the fines and reimbursements also

considered Genesco's violation of VIOR requirement No. 2. Yet, the Beierly memorandum does not reflect that Visa had any evidence to support this violation.

> Visa does agree that RDP contributed to the breach. Questions for TW:
> 1) Per PCI DSS requirement 2.3, all non-console administrative access must be encrypted. Did Genesco used VPN/SSH/SSL/TLS to encrypt RDP sessions? If not. Genesco was in violation of 2.3. This should have been documented on the forensic report and reflected on the PCI DSS Requirements Overview.

(Docket Entry No. 106 at 1-2) (emphasis in original). The language of the Beierly memorandum lacks any basis for this assertion about a Requirement 2.3 violation that Visa's VIOR requires for a determination to justify a fine or assessment. As provided in Visa's VIOR, Visa must have "[f[orensic confirmation or preponderance of evidence that a breach exists". (Docket Entry No. 135-1 at 8).

Moreover, as stated earlier, California law requires that Genesco's security breaches must be a "substantial factor" in the cause of Visa's purported losses. From the Court's perspective, discovery of Genesco's compliance with all of Visa's VIOR, CISP, or PCI-DSS requirements would cause unnecessary expense. Visa has not shown that its discovery requests directed to all VIOR rules would lead to the discovery of admissible evidence, if those provisions did not cause Visa's losses at issue. The "mend your hold" principle that California courts recognize, is an equitable doctrine and also counsels this limitation of discovery to the basis for Visa's assessments and fines because to do otherwise would not lead to the discovery of admissible evidence. This limitation is also consistent with Visa's VIOR that limits fines and assessments to facts known at the time by Visa. This limitation on discovery also promotes reasoned decision making in this important commercial system. This limitation is also analogous to the product line limitation in other contract actions cited in Moore's where discovery was limited to the product that caused the alleged breach of contract.

Whether as an application of California law or federal procedural law on discovery in breach of contract actions or based upon the parties' contract limiting assessments to the facts known to Visa, the Court concludes a limitation on the scope of discovery in this action is reasonable and necessary. Given that Trustwave's report was the basis for Visa's assessments and fines, the Court concludes that discovery should be limited to Genesco's alleged violations of Visa's VOIR, CISP and PCI-DSS computer system requirements as found by Trustwave, for which Visa imposed its assessments and fines. These violations, if any, would be the substantial cause of the compromise in Visa's system and Visa's purported losses. Thus, the Court concludes that discovery shall be limited to only the VIOR rules cited by Visa as the basis for its fines and reimbursements.

This Court is also mindful that the purpose of the rules is "to secure the just, speedy, and inexpensive determination of every action". Fed. R. Civ. P. 1. Amendments to the rules reflect that purpose. Without a formal discovery request, Rules 26(a)(1) requires disclosures of all persons with knowledge of discoverable matters and documents that a party relies upon for its claims and defenses. Fed. R. Civ. P. 26(a)(1)(A)(i). Other amendments to Rules 11, 16 and 26 were to control the costs of unfettered discovery. This purpose motivates this Court's Local Rule 16 on case management to tailor discovery to the needs of the particular case so as to avoid unnecessary discovery and its costs. Although the parties have ample financial resources, that fact does not justify unnecessary discovery. Moreover, Genesco's pleadings refer to the Visa rules that were the bases for the fines and assessments. Genesco does not seek a declaratory judgment that Genseco was in complete or full compliance with Visa's VIOR and other requirements.

Nothing in this ruling on Genesco's objections to relevancy and burdensomeness will deprive Visa of the necessary information. Genesco must disclose the identities of all persons in its employ

who may have knowledge of matters relating to the problems that gave rise to Visa's fines and assessment. Genesco must disclose the relevant documents upon which Genesco relies for its claims. Depositions of Genesco officials should provide additional detail. By rule and Case Management Order, Genesco must provide an expert report that must be presented as the direct testimony of its expert at trial with full disclosures of the opinions and bases for those opinions. Fed. R. Civ. P. 26(a)(2) and (Docket Entry No. 25, Case Management Order at 11). This Court's ruling limits Visa to the VIOR rules that Visa identified as violated by Genesco for which there was forensic evidence. The Court will allow Visa to make a particularized showing that discovery regarding other VIOR rule(s) is necessary as clearly related to the VIOR rule cited for Visa's assessment.

2. The Rule 407 Objection

Genesco next objects to Visa's discovery requests on changes to Genesco's computer system after the Intrusion, citing Federal Rule of Evidence 407 as barring admissibility of certain subsequent remedial measures. Genesco cites this rule as barring the discovery of this evidence citing Vardon Golf Co. v. BBMG Golf Ltd., 156 F.R.D. 641, 653 (N.D. Ill. 1994) (denying motion to compel discovery of subsequent remedial measures because the "evidence sought is not reasonably calculated to lead to the discovery of any other evidence but that relating to the culpability of Dunlop for allegedly infringing on the Raymont patent."); Kakule v. Progressive Cas. Ins. Co., 2008 WL 1902201 at *4-5 (E.D. Pa. April 30, 2008) (issuing protective order because information sought in deposition would be barred by Fed. R. Evid. 407).

Visa responds that Fed. R. Evid. 407 limits only the admissibility of certain evidence at trial, not discovery. Moreover, Fed. R. Evid. 407 does not apply to involuntary remedial measures. In re Aircrash in Bali, Indon., 871 F.2d 812, 817 (9th Cir. 1989) (FRE 407 not implicated when remedial

measures are involuntary) or where necessary to prove causation. Brazos River Auth. v. GE Ionics, Inc., 469 F.3d 416, 429 (5th Cir. 2006).

Any remedial measures that were taken by Genesco to comply with the Trustwave report must be produced by Genesco. The Trustwave report reflects remedial measures that Genesco was required to make and, in fact, implemented those remedial measures. Thus, for discovery purposes, as to Topic Nos. 19, 20, and 25 seeking information on Genesco's remediation of its security system based upon the Trustwave report, Genesco's objection is overruled, as "evidence of a party's analysis of its product," is discoverable. Brazos River Auth. v. GE Ionics, Inc., 469 F.3d 416, 430 (5th Cir. 2006) (quoting Prentiss & Carlisle Co. v. Koehring-Waterous Div. of Timberjack, Inc., 972 F.2d 6 (1st Cir.1992)). Yet, consistent with the Court's earlier ruling on relevancy, any other remedial changes that Genesco made to its computer system that were not required by the Trustwave report, are inappropriate for discovery.

3. The Privilege and Expert Discovery Issues

a. Consultant Expert

Here, Genesco objects to Visa's discovery requests and subpoena to the Stroz firm for the same materials because Genesco is not relying on Stroz's report or its Stroz consultant for evidence to support its claims in this action. Federal Rule of Civil Procedure 26(b)(4)(D) provides that "a party may not, by interrogatories or depositions, discover facts known or opinions held by an expert retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial." This "non-testifying expert" privilege is distinct from the work-product doctrine and the attorney-client privilege. In re PolyMedica Corp. Sec. Litig., 235 F.R.D. 28, 30 (D. Mass. 2006). Absent a showing of extraordinary circumstances,

this rule restricts discovery of facts known and opinions held by non-testifying experts and is designed to prevent the unfairness of counsel benefiting from an adversary's retention and financing of an expert. Vanguard Sav. & Loan Ass'n VSL Service Corp. v. Banks, No. Civ. A. 93-4627, 1995 WL 71293, *2 (E.D. Pa. Feb. 17, 1995); Sloan Valve Co. v. Zurn Indus., No. 10 C 204, 2012 WL 5499412, *2-*3 (N.D. Ill. Nov. 13, 2012).

As the District Court in Precision of New Hampton, Inc. v. Tri Component Products Corp., No. C12–2020, 2013 WL 2444047 (N.D. Iowa. June 05, 2013) summarized:

> A party seeking discovery of facts or opinions held by a non-testifying consulting expert bears the burden of showing exceptional circumstances. Hartford Fire Ins. Co. v. Pure Air On The Lake Ltd., 154 F.R.D. 202, 207–08 (N.D. Ind.1993). Courts have interpreted exceptional circumstances to mean that the party cannot obtain equivalent information from another source. In re Shell Oil Refinery, 132 F. R. D. 437, 442 (E.D. La.1990). For example, in In re Shell Oil, the court denied the plaintiff's request to see results of tests conducted by Shell because the plaintiffs could obtain the same information by using their own experts. Id. at 443. Similarly, in Sara Lee Corp. v. Kraft, the court found exceptional circumstances lacking where the party seeking discovery had retained an expert to testify on the same subject. Sara Lee Corp., 273 F.R.D. at 420.
>
> However, courts have found exceptional circumstances where the object or condition at issue cannot be observed by experts of the party seeking discovery. Hartford Fire Ins. Co., 154 F.R.D. at 208. For example, in Delcastor, Inc. v. Vail Associates, Inc., 108 F.R.D. 405, 409 (D.Colo.1985), the court found exceptional circumstances where only the defendant's expert had an opportunity to investigate the cause of a mud slide before conditions at the site changed. Id. The court noted that exceptional circumstances exist when "circumstances precluded all but one of the party's experts from gaining a first hand observation of the object of condition." Id.

Id. at *3. See also, Morningware, Inc. v. Hearthware Home Products, Inc., No. 09-c-4348, 2012 WL 3721350 at *6 (N.D. Ill. Aug. 27, 2012) ("Consulting experts do not offer testimonial evidence during a litigation proceeding, and parties are therefore not entitled to discovery from consulting experts.").

Although Visa characterizes its discovery of the Stroz firm as a fact witness for Stroz's work on Genesco's response to the Trustwave report, as stated above, Visa must establish extraordinary circumstances for this discovery. As to Visa's characterization of discovery of Stroz as fact discovery, in the Court's view, the Stroz representative would necessarily be applying his or her specialized knowledge. Thus, Visa's characterization of its Stroz discovery requests as involving a fact witness is inappropriate. To accept that characterization would effectively eviscerate and undermine the core purpose of Fed. R. Civ. P. 26(b)(4)(D). This Genesco objection is sustained.

b. Attorney Client and Work Product Privileges

Genesco next asserts the attorney client and work product privileges to bar Visa's discovery requests for Sisson's deposition and his records and communications during his investigation of the cyber attack and Visa's assessments and fines. Attorneys' factual investigations "fall comfortably within the protection of the attorney-client privilege." Sandra T.E. v. South Berwyn School Dist. 100 600 F.3d 612, 619 (7th Cir 2010) (citing Upjohn Co. v. United States, 449 U.S. 383, 394-99 (1981)). This privilege extends to the Stroz firm that assisted counsel in his investigation. United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961). There, the Second Circuit held that the attorney-client privilege extends to counsel's communications with agents and experts who are retained by counsel for the purpose of providing legal advice. In Kovel, the privilege extended to an accountant who was retained by counsel.

> Accounting concepts are a foreign language to some lawyers in almost all cases, and to almost all lawyers in some cases. Hence the presence of an accountant, whether hired by the lawyer or by the client, while the client is relating a complicated tax story to the lawyer, ought not destroy the privilege, any more than would that of the linguist in the second or third variations of the foreign language theme discussed above; the presence of the accountant is necessary, or at least highly useful, for the effective consultation between the client and the lawyer which the privilege is

designed to permit.

Id.

The work product privilege also attaches to an agent's work under counsel's direction. United States v. Nobles, 422 U.S. 225, 238-39 (1975) ("At its core, the work-product doctrine shelters the mental processes of the attorney, providing a privileged area within which he can analyze and prepare his client's case. But the doctrine is an intensely practical one, grounded in the realities of litigation in our adversary system. One of those realities is that attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial. It is therefore necessary that the doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself'") (footnote omitted). See also Fed. R. Civ. P. 26(b)(3). Sandra T. E. v. South Berwyn Sch. Dist. No. 100, 310 Fed. Appx. 927, 927 (7th Cir. 2010); In re Grand Jury Subpoena Dated Oct. 22, 2011, 282 F.3d 156, 161 (2d Cir. 2002).

Visa first asserts that Genesco did not file a privilege log describing any documents containing such privileged information and cites this Court's decisions in John B. v. Goetz, 879 F. Supp. 2d 787, 889, 893 (M. D. Tenn . 2010) and Etheredge v. Etheredge, No. 1:12-cv-165, 2013 WL 4084642 (M.D. Tenn. July 13, 2013). In the more recent decision, this Court stated:

> In other words, to assert any privilege, the Defendants had to prepare and serve a privilege log, and their failures to do so constitute waivers of these privileges. Carfagno v. Jackson National Life Ins., No. 5:99cv 118, 2001 WL 34059032 at * 2 (W.D. Mich. Feb 13, 2001) ("**Defendant's failure to provide the court with sufficient specificity to permit the court to determine whether the privilege asserted applies to the withheld documents provides an independent ground for finding a waiver of any privilege or immunity**") (citing inter alia United States v. Construction Prod. Research Inc., 73 F.3d 464, 473–74 (2d Cir.1996) and Smith v. Dow Chemical Co., 173 F. R. D. 54, 57–8 (W.D.N.Y.1997)). Moreover, "**the unjustified failure to list privileged documents on the required log of withheld documents in a timely and proper manner operates as a waiver of any applicable privilege**". Onebeacon Ins. Co. v. Forman Int'l. Ltd., No.04 Civ. 2271(RWS), 2006 WL 3771010 at * 7 (S. D. N. Y. Dec.15, 2006) (collecting numerous authorities).

> Here, **the Defendants' responses to Plaintiff's motion and to Plaintiff's discovery requests for similar information fail to provide any information to enable the Court to determine the appropriateness of the privileges asserted for information that the Defendants provided to Merrill Lynch**. Under Tennessee law, "[t]he attorney client privilege is not absolute, nor does it cover all communications between a client and his or her attorney". Boyd v. Comdata Network, Inc., 88 S.W.3d 203, 213 (Tenn. Ct. App. 2002).

Id, at ** 4, 5 (emphasis added). In Etheredge, the Court recognized the requirement of a privilege log or sufficient information to assess the privilege. There, the Court found waiver for lack of any information to assess the privilege issues.

For most actions, this Court requires a privilege log, but a study of the history of law reflects that most rules eventually give rise to exceptions where the facts warrant. Moreover, Rule 26(b)(4)(D) does not require a privilege log, only information that "describes the nature of the documents, communications, or tangible things not produced or disclosed- and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim." Rule 26(b)(5)(A)(ii) also does not require a privilege log. As the Supreme Court observed in a similar situation involving an issue of privilege for a corporate counsel's investigation: "The first step in the resolution of any legal problem is ascertaining the factual background and sifting through the facts with an eye to the legally relevant." Upjohn, 449 U. S. at 390-91.

Under the applicable case law and the facts here, the affidavits of Genesco's counsel and other documents provide an ample basis to assess the privilege issues raised by the parties' discovery motions.[5] Upjohn provides definitive and controlling guidance. There, corporate counsel for an

---

[5] Moreover, to disclose the details for a privilege log of documents exchanged between Sisson and Stroz would infringe upon Genesco's counsel and his consultant's mental processes that are entitled to absolute protection in this Circuit. Toledo Edison Co. v. G.A. Tech., Inc., 847 F.2d 335, 341 (6th Cir.1988) ("the court ... must 'protect against disclosure of mental impressions, conclusions, opinions on legal theories of an attorney or their representative.") See also Sandburg v. Virginia Bankshares, Inc., 979 F.2d 332, 355 (4th Cir.1992). Under Sporck v.

international company that was subject to a governmental investigation, prepared questionnaires for corporate managers and agents about the subject of that investigation. The managers and employees' responses "were to be sent directly to Thomas," the company's general counsel. 449 U.S. at 387. There, the government sought "All files[6] relative to the investigation conducted under the

---

Peil, 759 F.2d 312, 315-17 (3rd Cir.1985), that this Court has followed in prior decisions, a disclosure of a lawyer's selection of certain documents from a large amount of documents infringes on counsel's mental processes and disclosure of those processes would impair an attorney's preparations as disclosing counsel's strategies. Thus, to require a privilege log for the assertion of these privileges for Genesco's counsel and his agent, the Stroz firm, would itself violate the work product privilege.

[6] Here, Visa's document requests are similarly, if not more, comprehensive:

REQUEST FOR PRODUCTION No. 11: All DOCUMENTS relating to YOUR compliance or non-compliance with the CARDHOLDER ACCOUNT DATA SECURITY REQUIREMENTS, including without limitation any and all internal reports and external COMMUNICATIONS, for the time period from January 1, 2007 to present.

REQUEST FOR PRODUCTION No. 12: All COMMUNICATIONS relating to YOUR compliance or non-compliance with the CARDHOLDER ACCOUNT DATA SECURITY REQUIREMENTS, including without limitation any and all internal and external COMMUNICATIONS, for the time period from January 1, 2007 to present.

REQUEST FOR PRODUCTION No. 15: All DOCUMENTS related to the INTRUSION, including but not limited to any investigation by YOU (or on YOUR behalf) relating to the INTRUSION or any COMMUNICATIONS by YOU relating to the INTRUSION.

REQUEST FOR PRODUCTION No. 16: All DOCUMENTS related to the PERSON(S) that provided YOU with any component or services in connection with the GENESCO PAYMENT PROCESSING NETWORK in use during the INTRUSION through the present time.

REQUEST FOR PRODUCTION No. 17: All COMMUNICATIONS involving YOU and any third party discussing or referencing forensic information or any investigation related to the INTRUSION.

REQUEST FOR PRODUCTION No. 30: All COMMUNICATIONS related to the INTRUSION, including but not limited to any investigation by YOU (or on YOUR behalf) relating to the INTRUSION.

supervision of Gerard Thomas", the general counsel. Upjohn, 449 U.S. at 387. The Supreme Court ruled that "communications by Upjohn employees to counsel are covered by the attorney-client privilege disposes of the case so far as the responses to the questionnaires and any notes reflecting responses to interview questions are concerned." Id. at 397

As to the general counsel's notes and memoranda on that investigation, the Supreme Court stated: "The notes and memoranda sought by the Government here, however, are work product based on oral statements. If they reveal communications, they are, in this case, protected by the attorney-client privilege. To the extent they do not reveal communications, they reveal the attorneys' mental processes in evaluating the communications". Id. at 401.

In this Circuit, a five-step analysis is employed to determine whether the work product doctrine applies. Toledo Edison Co. v. G.A. Tech., Inc., 847 F.2d 335, 339 (6th Cir.1988).

> When a claim that materials have been "prepared in anticipation of litigation or for trial" is made, the court must go through the sequential steps set out in Fed.R.Civ.P. 26(b)(3) as follows:
>
> 1. The party requesting discovery must first show that, as defined in Rule 26(b)(1), the materials requested are "relevant to the subject matter involved in the pending litigation" and not privileged. Because the application of subdivision (b)(3) is limited to "documents and tangible things otherwise discoverable under subdivision (b)(1)," the burden of making this showing rests on the party requesting the information. In this case it is Torrey Pines.

REQUEST FOR PRODUCTION No. 31: All COMMUNICATIONS between YOU and the PERSON(S) that provided YOU with any component or any service in connection with the GENESCO PAYMENT PROCESSING NETWORK in use during the INTRUSION through the present time.

(Docket Entry No. 120 at 2, 5, 6, 8-11).

In the Court's view, Visa's discovery requests seek to "drain the pond and collect the fish from the bottom. This exercise goes beyond the bounds set by the discovery rules." In re IBM Peripheral EDP Devices Antitrust Litigation, 77 F. R. D. 39, 42 (N. D. Cal. 1977).

2. If the party requesting discovery meets this burden and the court finds that the claimed material is relevant and not privileged, the burden shifts to the objecting party to show that the material was "prepared in anticipation of litigation or for trial" by or for that party or that party's representative, including that party's attorney, consultant, surety, indemnitor, insurer or agent. This showing can be made in any of the traditional ways in which proof is produced in pretrial proceedings such as affidavits made on personal knowledge, depositions, or answers to interrogatories. This showing can be opposed or controverted in the same manner. The determination of this matter is the second sequential determination that must be made by the court.

3. If the objecting party meets its burden as indicated above and the court finds that the material was prepared in anticipation of litigation or for trial by one of the persons named in the rule, the burden shifts back to the requesting party to show that the requesting party (a) has substantial need of the materials in preparation of the party's case, and (b) that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In doing this, attention is directed at alternative means of acquiring the information that are less intrusive to the lawyer's work and whether or not the information might have been furnished in other ways.

4. After the application of the shifting burdens, even if the court determines that the requesting party has substantial need of the materials in the preparation of its case and that the requesting party is not able, without undue hardship, to obtain the substantial equivalent of the materials by other means, the rule flatly states that the court is not to permit discovery of "mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of the party concerning the litigation." On this issue, the burden of showing that the nature of the materials are mental impressions, conclusions, opinions or legal theories of an attorney or representative, rests on the objecting party. The term "representative of the party" embraces the same persons as did the term "party's representative" set out earlier in the rule including "... consultants ... agent...."

5. The court may not order discovery of materials if discovery of such materials would violate Rule 26(b)(4) involving trial preparation, i.e., experts. Different standards and procedures are set forth because of the nature of experts and the different purposes for which they are employed. Experts are used by parties for different purposes just as information is prepared or acquired by parties for different purposes. Experts may be used to assist in the operation of a machine or a procedure or to repair or improve it, or they may be employed to assist in preparation for trial or to give testimony at the trial. Rule 26(b)(4) specifically and exclusively deals with the standards and methods of discovery of facts known and opinions held by experts acquired or developed in anticipation of litigation or for trial. Subdivision (b)(4) does

> not apply to facts known or opinions held by experts not acquired or developed in anticipation of litigation or for trial. If it is shown that the facts or opinions of the expert were so acquired the standards and procedures of subdivision (b)(4) apply. Because material covered by subdivision (b)(3) and (b)(4) often overlap, it may be necessary for the court to continue with the (b)(4) analysis.

Id. at 339-40.[7]

These privileges arise from the relationship between Genesco and the Stroz firm for which Genesco's affidavits are appropriate and sufficient to enable the Court to decide whether the privilege attaches. Visa has shown the relevance of the Sisson and Stroz documents as Genesco's responses to the Trustwave report and the Visa fines and assessments. Genesco's affidavits satisfy that the Stroz firm was retained in contemplation of litigation, as reflected in the express language of the retainer agreement.

This Court and other courts require a privilege log for most cases, but here given the international scope of this controversy and the circumstances of the retention of a consultant computer expert to assist Genesco's counsel in a complex computer investigation, this action fits squarely within Upjohn. Given that this controversy involves Genesco's retail establishments through the world, the individual listing of each document to Genesco's counsel for determining privilege seems impracticable and unnecessary to decide this privilege issue in light of Upjohn. The Court, however, will require a privilege log for any document that was prepared by a Genesco employee, but was not addressed directly to Genesco's counsel as such factual circumstances fall outside of Upjohn. Genesco also cannot withhold documents prepared in its ordinary business, as

---

[7] A bright line rule of disclosure applies to testifying experts, Regional Airport Authority of Louisville v. LFG, LLC, 460 F.3d 697, 714 (6th Cir. 2006), but the privilege here involves a consultant expert.

reflected by the Court's ruling that remedial measures that Genesco took in response to Trustwave's report must be produced because the Trustwave report reflects that those measures were undertaken in the ordinary course of business, not for Genesco's counsel.

Moreover, "[a]s Rule 26 and Upjohn make clear, these privileges "cannot be disclosed simply on a showing of substantial need and inability to obtain the equivalent without undue hardship." Id. at 401. In Nationwide Mut. Ins. Co. v. Home Ins. Co., 278 F.3d 621, 628 (6th Cir. 2002), the Sixth Circuit adopted the Eighth Circuit's decision in Shelton v. Am. Motors Corp., 805 F.2d 1323, 1327 (8th Cir. 1986), that to overcome the attorney client privilege, Visa must show that: "(1) no other means exist to obtain the information; (2) the information sought is relevant and nonprivileged [sic]; and (3) the information is crucial to the preparation of the case."

As to these factors, the subjects of the Stroz subpoena and the Sisson deposition notice are relevant, but are privileged. Genesco also cites its production of over 80,000 pages of documents, answers to 42 interrogatories, 36 responses to requests for admission, and five Genesco employees deposed for more than 20 hours over four days on every topic relevant to Visa's defense of Genesco's claims. Moreover, Visa has served subpoenas on numerous third parties, including both Acquiring Banks, Trustwave, and the former Trustwave employee who had principal responsibility for the forensic investigation of Genesco's system. The Court concludes that Visa has not shown that there are not other means to acquire relevant information other than discovery of Stroz, Genesco's consultant and Sisson. In fact, the Trustwave report and analysis of Genesco's computer system was provided to Visa and this Court has ordered Genesco to provide the remedial measures taken by Genesco in response of Trustwave's report.

Visa relies upon Visteon Global Techs., Inc. v. Garmin Int'l, Inc., 903 F. Supp. 2d 521 (E.D.

Mich. 2012), where defendant's in-house counsel directed the defendant's employee, an engineer, on modifications of the defendant's product's design to avoid infringement of the plaintiff's patents. The engineer testified that he was unable to answer certain questions and "continually asserted that he was simply carrying out the directives" of in-house counsel. Id. at 529. There, the district court permitted plaintiff to depose opposing counsel "within the confines of the Shelton rule." Id. at 531. The Court deems Visteon factually inapposite in that Genesco's expert will be required to provide all of the bases for Genesco's rebooting or other theory of recovery. In sum, neither Sisson nor Stroz is "the only other [defense] witness with knowledge regarding the design around process." Id.

As to Visa's contentions on Genesco's waiver of these privileges by disclosing the Stroz report to Visa and filing Sisson's affidavits, in March 2011, Genesco provided to Visa (and others) an annotated response to the Trustwave Report, disputing Trustwave's findings and clearly reflecting analysis and evaluation of Genesco's PCI DSS compliance. Genesco contends that brief references to its privileged investigation conducted by attorneys do not constitute a waiver of attorney client privilege, especially where, as here, those references do not describe opinions, analysis or bases for legal reasoning.

To be sure, a client may waive the attorney-client or work product privilege "by conduct which implies a waiver of the privilege or a consent to disclosure." Reitz v. City of Mt. Juliet, 680 F. Supp. 2d 888, 892 (M.D. Tenn. 2010) (citations omitted). In TJX Companies Data Security Breach Litig., Case No. 07-cv-10162-WGY (D. Mass. Nov. 9, 2007), the District Court held that the non-testifying expert, attorney-client, and work product privileges prevented such discovery,

notwithstanding the fact that the investigator had communicated with third parties.[8] Sloan Valve Co., No. 10 C 204, 2012 WL 5499412 at *3 (N. D. Ill. Nov. 13, 2013) (granting motion for protective order barring defendants from taking deposition of non-testifying expert, holding that party instead could pursue discovery of the contentions via expert discovery, and pointing party seeking discovery to the Court's case management schedule, which fixes the date until which the party must wait for expert disclosures). In factually similar circumstances, Precision of New Hampton, Inc. v. Tri Component Products Corp., No. C12-2020, 2013 WL 2444047 (N.D. Iowa June 5, 2013), "[t]he court found it immaterial that the plaintiff may have voluntarily disclosed the expert report to third parties, and stressed that the only relevant question is whether the plaintiff meets the requirements of Rule 26(b)(4)(B)." (citations omitted). See also K & S Assocs. v. Am. Ass'n of Physicists in Med., No. 3:09-01108, 2011 WL at 249361, at *4 (M. D. Tenn. Jan. 26, 2011) (two references to an internal investigation memorandum insufficient to constitute waiver) (citation omitted).

Based upon Precision of New Hampton, the Court concludes that there is not any waiver of the attorney client privilege. Assuming a waiver based upon disclosure of the Stroz report, the limitation on the nontestifying expert consultant would still bar the Stroz discovery, as that protection arises under Rule 26(b)(D)(4) that serves different purposes and does not permit of waiver. Precision of New Hampton, Inc., 2013 WL 2444047, at *3 ("where a party enjoys protection under Rule 26(b)(4)(D), the protection is not subject to waiver.").

For these reasons, the Court concludes that Genesco's motion for a protective Order (Docket Entry No. 88) should be granted in part and denied in part; Visa's motion to compel (Docket Entry

---

[8]See Affidavit of Seth C. Harrington dated October 30, 2013 (Docket Entry No. 192, Harrington Affidavit at ¶¶ 5-7 and Exhibit Nos. 1 and 2 thereto).

No. 120) should be granted in part and denied in part and Genesco's motions for protective order concerning Visa's subpoena to Genesco's expert consultant and Visa's deposition notice for Genesco's general counsel (Docket Entry Nos. 201 and 235) should be granted.

An appropriate Order is filed herewith

ENTERED this the 17th day of January, 2014.

William J. Haynes, Jr.
Chief United States District Judge

ame pro tem
3-10-14